proofpoint.

GDPR READINESS: DIGITAL FOOTPRINT DISCOVERY AND PROTECTION

This guide outlines basic provisions of the new General Data Protection Regulation (GDPR) and how it applies to your digital footprint—even if you're outside of the European Union (EU). You'll learn why identifying and protecting digital properties that collect personal data is critical. And you'll get a roadmap of how to be ready to comply with GDPR mandates.

GDPR HIGHLIGHTS

1 AFFECTED COMPANIES

If your business handles the personal data of EU residents, you are subject to GDPR. It applies even if your business is located outside the EU.

2 MAIN PURPOSE

The GDPR aims to protect all EU residents from data and privacy breaches. It harmonizes data privacy laws across all European Union member states.

3 THE PRIMARY NEED

Before GDPR, each country in the EU had its own data protection laws. So doing business in the EU meant dealing with different laws for each country. GDPR give firms one consistent regulation for data privacy.

4 EFFECTIVE DATE

GDPR was adopted on 27 April 2016. It goes into effect on 25 May 2018. Organizations must be ready to show compliance by that date.

> “Our digital future can only be built on trust. Everyone’s privacy must be protected. Strengthened EU data protection…is a major step forward and we are committed to making it a success for everyone.”

ANDRUS ANSIP

EU COMMISSION VP
FOR THE DIGITAL SINGLE MARKET

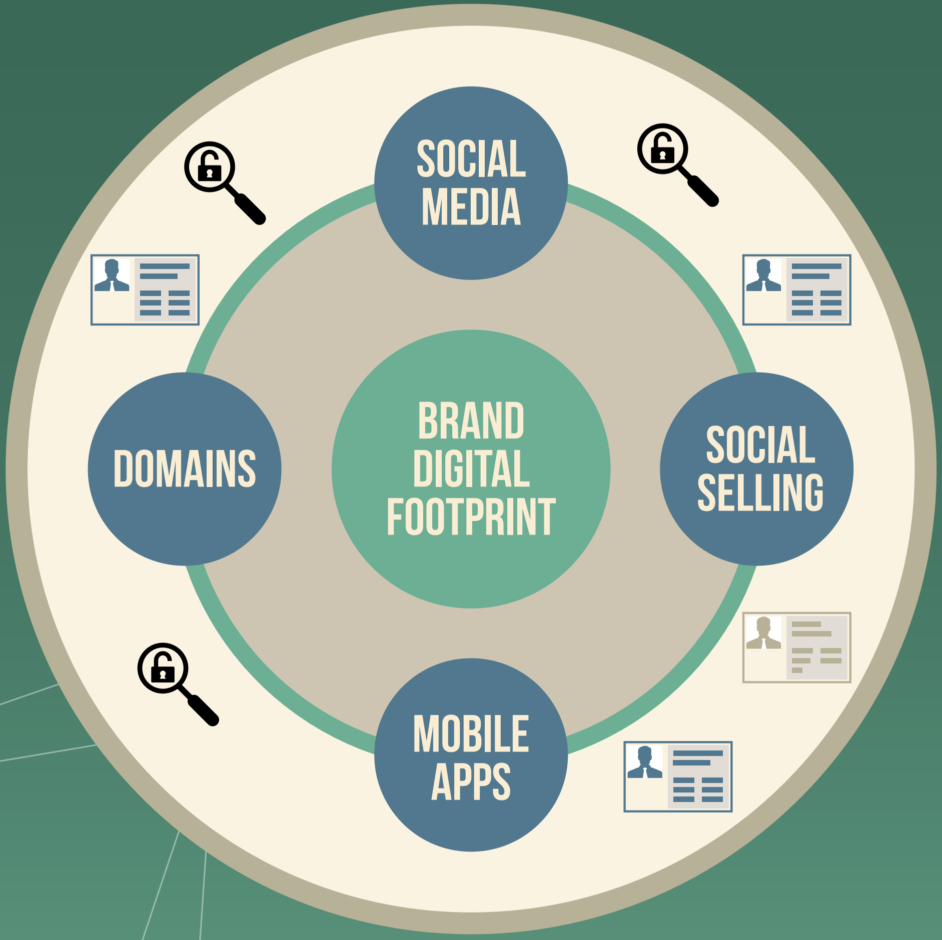
GDPR AND YOUR DIGITAL FOOTPRINT

As you prepare to meet GDPR requirements, monitoring and securing your digital footprint is critical. Your company's digital footprint includes all internet-based digital channels, including:

- Social media
- Social selling
- Internet domains
- Mobile apps

Your digital channels are external assets that may collect and store personal data. These include:

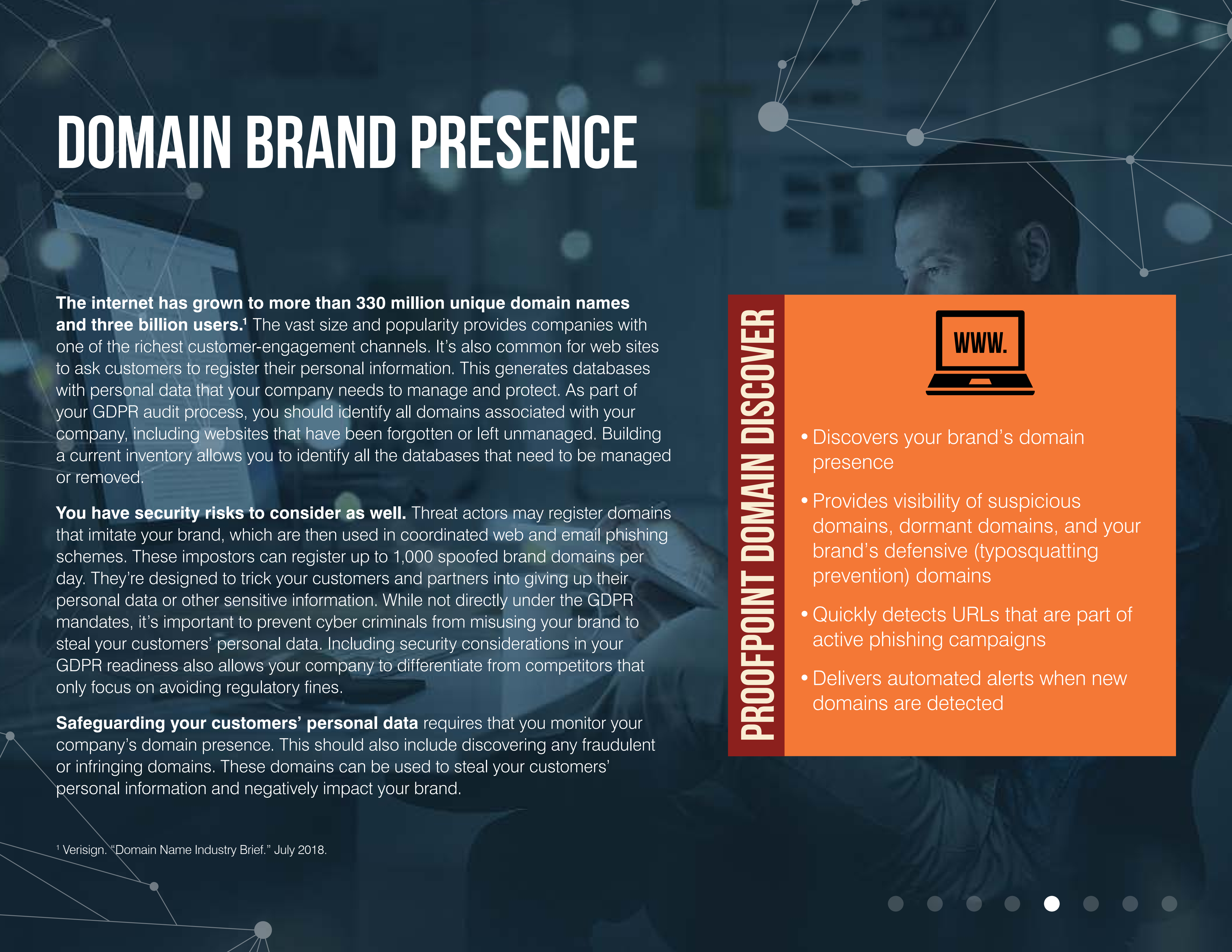
- Users' names
- Social-media presence
- Profile information
- Location data
- Phone number
- Birthdate
- And more.



In addition to identifying and managing EU-resident personal data across your digital footprint, it's also important to protect the data from a security breach, which leads to a misuse of personal data. Criminals masquerade as your brand, across digital channels, to bait your customers with phishing attacks to steal their personal data and login credentials.

Proofpoint Digital Risk Protection discovers your digital presence and protects against security, brand, and compliance risks across web, mobile, and social media. It's the only solution that gives you a holistic approach to address digital risk challenges associated with GDPR compliance by:

- Discovering your brand's digital presence, including fraudulent and unauthorized brand elements
- Automating compliance content scanning and enforcement to discover personal data and GDPR compliance risks
- Securing against account takeovers, digital brand fraud, and phishing attacks on your customers



DOMAIN BRAND PRESENCE

The internet has grown to more than 330 million unique domain names and three billion users.[1] The vast size and popularity provides companies with one of the richest customer-engagement channels. It's also common for web sites to ask customers to register their personal information. This generates databases with personal data that your company needs to manage and protect. As part of your GDPR audit process, you should identify all domains associated with your company, including websites that have been forgotten or left unmanaged. Building a current inventory allows you to identify all the databases that need to be managed or removed.

You have security risks to consider as well. Threat actors may register domains that imitate your brand, which are then used in coordinated web and email phishing schemes. These impostors can register up to 1,000 spoofed brand domains per day. They're designed to trick your customers and partners into giving up their personal data or other sensitive information. While not directly under the GDPR mandates, it's important to prevent cyber criminals from misusing your brand to steal your customers' personal data. Including security considerations in your GDPR readiness also allows your company to differentiate from competitors that only focus on avoiding regulatory fines.

Safeguarding your customers' personal data requires that you monitor your company's domain presence. This should also include discovering any fraudulent or infringing domains. These domains can be used to steal your customers' personal information and negatively impact your brand.

PROOFPOINT DOMAIN DISCOVER

- Discovers your brand's domain presence
- Provides visibility of suspicious domains, dormant domains, and your brand's defensive (typosquatting prevention) domains
- Quickly detects URLs that are part of active phishing campaigns
- Delivers automated alerts when new domains are detected

[1] Verisign. "Domain Name Industry Brief." July 2018.

SOCIAL MEDIA AND SOCIAL SELLING BRAND PRESENCE

Social media is a great way to promote your products and interact with customers. Consumers turn to social media to engage with their favorite brands with 74% relying on social media to guide their purchases.[2] As your social presence and fan base grows so too does your exposure to personal data compliance and security risks that you need to manage. The average brand has 320 social media accounts. With so many accounts, corporate governance and compliance can get complex.

And then there are your brand ambassadors' personal social media accounts. It's important that your social selling program doesn't hurt your brand or introduce compliance violations with GDPR. Organizations need to ensure social selling interactions don't share personal data or private conversations that could present a data protection risk.

Also, you need to consider the security risks from fraudulent brand accounts set up to phish your customers' personal data and credentials. This poses a big risk to your customers and negatively impacts your brand reputation. In fact, a Proofpoint study reported social media phishing links grew 70%, and fake customer-support accounts used for phishing jumped 30% from Q3–Q4 in 2017. [3]

PROOFPOINT SOCIAL MEDIA PROTECTION

- Automates social account discovery, content monitoring, and compliance policy enforcement
- Applies policy controls that automate personal data and other content remediation
- Monitors social platforms for fraudulent accounts that impersonate your brand
- Prevents phishing, malware, and other attacks on your customers and followers
- Ensures social selling profile accounts are compliant
- Supervises social selling posts for harmful content and compliance risks

[2] MarkMonitor. "Brand Abuse Lurking on Social Media." October 2015.

[3] Proofpoint. "Q2 2017 Quarterly Threat Report." August 2017.

MOBILE APP BRAND PRESENCE

Today's mobile app ecosystem is large and dynamic. Users can download apps from hundreds of app stores. Google Play alone offers 3.6 million apps.[4] Mobile apps frequently request and store sensitive customer personal data, which falls within the scope of GDPR.

Mobile apps are also fertile ground for cyber criminals looking to impersonate your company and attack the people who trust it. According to Marketing Science, 40% of mobile app inventory is fraudulent.[5] Even if you don't have an official mobile app presence, you need to safeguard your customers against the risk of unsanctioned brand apps.

Keeping track of your mobile app presence and identifying fraudulent brand apps is a key part of safeguarding your customer personal data and protecting your digital footprint.

PROOFPOINT MOBILE DISCOVER

- Discovers your brand's mobile app presence with just a few clicks
- Identifies official brand apps that have bypassed security testing
- Continuously scans for fraudulent and unsanctioned apps
- Alerts you when new apps are detected

[4] AppBran. "Number of Android applications." February 2018.

[5] MobileAppDaily. "Here Are The Ways To Identify Mobile Ad Fraud." February 2018.

SUMMARY

For most organizations, GDPR is a game-changer. Getting compliance-ready should be top of mind for businesses and security leaders. That means prioritizing new programs and solutions that ensure your digital footprint is ready for the new rules.

Proofpoint Digital Risk Protection discovers and protects your brand's digital assets, allowing you to identify compliance exposures and reduce your organization's digital attack surface.

LEARN MORE: PROOFPOINT.COM/GDPR

proofpoint.

LEARN MORE

PROOFPOINT.COM/GDPR

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.